ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Number Theory 106 (2004) 187–199

JOURNAL OF Number Theory

http://www.elsevier.com/locate/jnt

Cohen–Lenstra heuristics and the Spiegelungssatz; function fields

Yoonjin Lee*

Department of Mathematics, Clark Science Center, Smith College, Northampton, MA 01063, USA

Received 19 November 1999; revised 23 September 2003

Communicated by D. Goss

Abstract

In this paper, we study the compatibility of Cohen–Lenstra heuristics with Leopoldt's Spiegelungssatz (= the reflection theorem) in the case of cyclic function fields. First, we prove a group-theoretical version of the Spiegelungssatz for cyclic function fields. Then we show the internal consistency of the function field analogue of Cohen–Lenstra heuristics in the case of cyclic function fields. It thus supports the validity of Cohen–Lenstra heuristics in function fields.

MSC: primary 11R29; secondary 11Sxx, 11Rxx

Keywords: Class groups; Cohen–Lenstra heuristics; Spiegelungssatz; Cyclic function field

Introduction

Cohen and Lenstra's conjectures provide us with very satisfactory answers to many questions about class groups. However, their conjectures have not been proved except in a few cases. In order to support Cohen and Lenstra's conjectures, Dutarte [2] showed in 1984 that the conjectural probabilities on the 3-rank of the class groups of quadratic fields are compatible with Scholz's theorem, a special case of the Spiegelungssatz. Dutarte showed the compatibility, assuming probabilistic independence and a law of equiprobability concerning the behavior of units. This

*Fax: +1-413-585-3786.

E-mail address: yjlee@smith.edu.

0022-314X/$ - see front matter
doi:10.1016/j.jnt.2004.01.001

compatibility confirms the internal consistency of Cohen–Lenstra's conjectures and hence supports the validity of their conjectures.

In [6], Dutarte's work is generalized to every odd prime p; it is proved that the conjectural probabilities on the p-rank of the class group of a quadratic field and the p-rank of a certain subgroup of the class group of a cyclic extension of degree $p-1$ of $\mathbb{Q}$ are compatible with the Spiegelungssatz for every odd prime p. Furthermore, it is proved that the Spiegelungssatz is compatible with the conjectural probabilities on the p-rank of certain subgroups of the class group of a cyclic extension of degree q of $\mathbb{Q}$, where q is a prime number dividing $p-1$.

Friedman and Washington [3] proposed in 1987 a conjecture that explained Cohen–Lenstra heuristics for the function field analogue of the set of imaginary quadratic fields. Yu [11] showed that one of the conjectural statements made by Friedman and Washington is true in an asymptotic sense for both imaginary and real function fields. Friesen [4] proved that a special case of Cohen–Lenstra heuristics in function fields is true as well. These support the function field analogue of the Cohen–Lenstra heuristics. Furthermore, Rosen [10] proved a function field version of a special case of Leopoldt's Spiegelungssatz and an application to hyper-elliptic function fields.

The question naturally arises whether or not the compatibility in the number field situation is also true in the function field situation. In this paper we answer this question: In Section 2, we prove a group-theoretical version of the Spiegelungssatz in cyclic function fields. Then it is applied to show the internal consistency of Cohen–Lenstra heuristics in the real cyclic function field case and the imaginary cyclic function field case (Section 3). The compatibility between the Spiegelungssatz and conjectural statements (obtained from Cohen–Lenstra heuristics in function fields) confirms the internal consistency of the function field analogue of Cohen–Lenstra heuristics. Thus, it supports the validity of Cohen–Lenstra heuristics in function fields.

This paper is based on my doctoral dissertation, directed by Dr. Michael Rosen, and written at Brown University. In [6], we discuss the same questions with respect to number fields, and we prove that the compatibility is true in the number field situation as well.

1. A function field analogue of the Spiegelungssatz

In this section we discuss a function field version of Leopoldt's Spiegelungssatz (= the reflection theorem) [7].

We introduce some notations. Let K be an algebraic function field of one variable with a finite constant field $\mathbb{F}$. We denote by q the number of elements in $\mathbb{F}$. Let S_∞ be a non-empty finite set of prime divisors of K; the elements in S_∞ are to be thought of as the primes at infinity. Let A be the ring of elements in K whose only poles are in S_∞; A is a Dedekind domain and its class group $Cl(A)$ is finite; the unit group of A (we will call it the unit group of K), denoted by E_K, is finitely generated of rank $s-1$, where $s = |S_\infty|$ (refer to [9] for details).

Let K_{sep} be a separable closure of $K, L \subset K_{\text{sep}}$ and $[L:K]$ be finite. Let B be the integral closure of A in L and $S_\infty(L)$ be the set of all prime divisors of L which lie above those in S_∞. B is also described as the set of elements of L whose only poles are in $S_\infty(L)$. The triple L, B and $S_\infty(L)$ is analogous to an algebraic number field, its ring of integers and its primes at infinity.

Definition 1.1. The Hilbert class field of K with respect to A, denoted by K^A, is the maximal unramified abelian extension of K in K_{sep} in which every prime in S_∞ splits completely.

To state some important results proved by Rosen [10], we begin with some results of the class field theory. Let $H \subset K_{\text{sep}}$ be the maximal unramified abelian extension of K and $\bar{K} \subset H$ the maximal constant field extension of K. Let $\mathscr{D}$ be the set of divisors of K. The Artin symbol $(\ , H/K)$ maps $\mathscr{D}$ onto the subgroup $Gal(H/K)^*$ of $Gal(H/K)$ consisting of automorphisms σ whose restriction to $\bar{K}$ is an integral power of the Frobenius automorphism φ ($\varphi \in Gal(\bar{K}/K)$ is characterized by $\varphi(\alpha) = \alpha^q$ for all constants α in $\bar{K}$). More precisely, we have

$$(\mathscr{D}, H/K)(a) = \varphi^{\deg \mathscr{D}}(a) \quad \text{for all } a \in \bar{K}.$$

Theorem 1.2. *$[K^A : K]$ is finite. The Artin symbol $(\ , K^A/K)$ induces an isomorphism*

$$Cl(A) \simeq Gal(K^A/K).$$

The constant field of K^A is $\mathbb{F}_\delta$, where δ is the greatest common divisor of $\{\deg P_1, \deg P_2, \ldots, \deg P_s\}$ when $S_\infty = \{P_1, P_2, \ldots, P_s\}$, and $\mathbb{F}_\delta$ is the unique subfield of $\bar{K}$ of dimension δ over $\mathbb{F}$.

Lemma 1.3. *If L/K is a Galois extension, so is L^B/K.*

Definition 1.4. If K, A, and S_∞ is our base triple, which is defined as before, then a separable extension of function fields L/K is said to be *totally real* if every prime in S_∞ splits completely in L. A separable extension L/K is called *totally imaginary* if every prime in S_∞ has only one prime above it in L.

As usual, let a triple K, A, and S_∞ be given, L/K be a finite abelian extension and B be the integral closure of A in L. Let l be a prime number different from the characteristic of K and $G = Gal(L/K)$. We assume that the exponent of G divides $l-1$ and $\zeta_l \in L$, where ζ_l is a primitive lth root of unity.

If χ is an irreducible character of G, then define the field L_χ to be the fixed field of the kernel of χ acting on L. Let B_χ be the integral closure of A in L_χ. Furthermore, let $E_\chi^o \subset E_{L_\chi}$ be the group of primary units in B_χ: A primary unit in B_χ is defined to be an element $u \in E_{L_\chi}$ such that $L(\sqrt[l]{u})/L$ is unramified everywhere and splits completely at primes above ∞ (i.e. primes in $S_\infty(L)$).

The character group $\hat{G}$ of G can be identified with Hom $(G, \mathbb{F}_l^*)$. Define $\eta \in \hat{G}$ by the formula $\sigma(\zeta_l) = \zeta_l^{\eta(\sigma)}$ for all $\sigma \in G$. For $\chi \in \hat{G}$, we define $\chi' = \eta\chi^{-1}$, the reflection character of χ. Note that $(\chi')' = \chi$.

If C is an abelian group, the l-rank of C is defined to be the dimension over $\mathbb{F}_l$ of C/C^l. We denote the ideal class group of B_χ (simply, called the class group of L_χ) by Cl_{L_χ}. Let r_χ be the l-rank of $(Cl_{L_\chi})_\chi$ and δ_χ be the l-rank of $(E_\chi^o)_\chi$, where $(Cl_{L_\chi})_\chi$ (resp. $(E_\chi^o)_\chi$) denotes $\varepsilon_\chi Cl_{L_\chi}$ (resp. $\varepsilon_\chi E_\chi^o$) and ε_χ is the idempotent corresponding to the character χ, given by $\varepsilon_\chi = \frac{1}{|G|}\sum_{\sigma \in G}\chi(\sigma)\sigma^{-1}$.

A function field version of the Spiegelungssatz is as follows (for a proof, refer to [10]).

Theorem 1.5. $-\delta_{\chi'} \leqslant r_{\chi'} - r_\chi \leqslant \delta_\chi$.

2. The Spiegelungssatz in the case of cyclic function fields

The main result of this section is Theorem 2.3, and the result is a group-theoretical version of the Spiegelungssatz in the case of cyclic function fields. Theorem 2.3 is a key result for showing the internal consistency of the Cohen–Lenstra heuristics concerning m-ranks of ideal class groups of cyclic function fields for some m in Section 3.

Let d be a prime number such that $d|q-1$ and choose a prime number m dividing $\frac{q^d-1}{q-1}$; d is the order of q mod m since $q^d \equiv 1 \pmod m$ and $d \mid m-1$. Then $K(\zeta_m)$ is a cyclic extension of dimension d over K. In fact, $\mathbb{F}(\zeta_m) = \mathbb{F}_{q^d}$. Since $d|q-1$, a primitive dth root of unity $\zeta_d \in \mathbb{F}^\times$; by Kummer theory, $\mathbb{F}_{q^d} = \mathbb{F}(\beta)$ for some β such that $\beta^d \in \mathbb{F}$, so that $K(\zeta_m) = K(\beta)$.

We will find the exact β since we need to know the Galois action on β. Let $\beta = \sum_{i=0}^{d-1} \zeta_d^i \zeta_m^{q^i}$ (We will show that $\beta \neq 0$ for some ζ_d shortly). It is easy to show that $\beta^q = \zeta_d^{-1}\beta$; thus, $\beta \notin \mathbb{F}$ since β is not fixed by $Gal(K(\zeta_m)/K)$(which is generated by the Frobenius map $\varphi(x) = x^q$). Furthermore, $(\beta^d)^q = \beta^d$, so $\beta^d \in \mathbb{F}$. Let n be β^d, i.e. $\beta = \sqrt[d]{n}$. Then, $K(\zeta_m) = K(\sqrt[d]{n})$.

Claim that $\beta \neq 0$ for some ζ_d. Let $C_{\zeta_d} = \sum_{i=0}^{i=d-1} \zeta_d^i \zeta_m^{q^i}$ and μ_d be the set of all dth roots of unity. To show that $S = \sum_{\zeta_d} \zeta_d^{-j} = 0$ for any $1 \leqslant j \leqslant d-1$, take $\omega \in \mu_d$, which is not equal to 1. Then $\omega^j S = \sum_{\zeta_d \in \mu_d} (\omega\zeta_d)^j = \sum_{\zeta_d \in \mu_d} (\zeta_d)^j = S$, which implies $(\omega^j - 1)S = 0$. Therefore, $S = 0$.

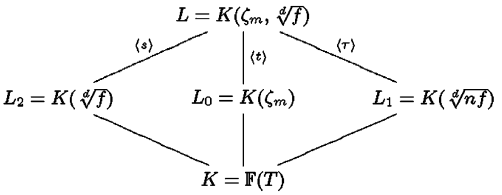
Multiplying C_{ζ_d} by ζ_d^{-r} for $r = 1, 2, \ldots, d-1$ and summing over all dth roots of unity, we obtain $\sum_{\zeta_d \in \mu_d} (\zeta_d^{-r} C_{\zeta_d}) = d\zeta_m^{q^r}$, since $\sum_{\zeta_d} \zeta_d^{-j} = 0$ for any $1 \leqslant j \leqslant d-1$. Then $\zeta_m^{q^r} = d^{-1}\sum_{\zeta_d \in \mu_d} (\zeta_d^{-r} C_{\zeta_d})$, since the characteristic of $\mathbb{F}$ is relatively prime to d.

If we assume that $C_{\zeta_d} = 0$ for every primitive dth root of unity ξ, then $\zeta_m^{q^r} = d^{-1}C_1$. Therefore, $\zeta_m^{q^r}$ have the same values for $1 \leqslant r \leqslant d-1$, which contradicts the fact that d

is the smallest such that $\zeta_m^{q^d}=1$. Consequently, C_{ζ_d} is not equal to 0 for some primitive dth root of unity ζ_d; we take it for β.

Let $f\in A=\mathbb{F}[T]$ be a monic dth power-free polynomial of degree divisible by $d, L_2=K(\sqrt[d]{f}), L_0=K(\zeta_m), L_1=K(\sqrt[d]{nf})$ and L be the compositum of L_1 and L_2, i.e. $L=K(\sqrt[d]{f},\zeta_m)$.

$Gal(L/K)\simeq\mathbb{Z}/d\mathbb{Z}\oplus\mathbb{Z}/d\mathbb{Z}$; $Gal(L/K)$ is abelian and the exponent of $Gal(L/K)$, namely d, divides $m-1$; hence, every irreducible m-adic character of $Gal(L/K)$ is 1-dimensional.



$Gal(L/L_2)\simeq Gal(\mathbb{F}(\zeta_m)/\mathbb{F})=\langle s\rangle$,

where s is a homomorphism defined by $s(\zeta_m)=\zeta_m^q$ and is of order d.

Let t be a map such that $t(\sqrt[d]{f})=\zeta_d\sqrt[d]{f}$; then $Gal(L/K(\zeta_m))\simeq Gal(K(\sqrt[d]{f})/K)=\langle t\rangle$. Taking $\tau=st$, we have $Gal(L/L_1)=\langle\tau\rangle$. Let η be a cyclotomic character $\eta: Gal(L/K)\to(\mathbb{Z}/m\mathbb{Z})^*$ such that $\eta(s)=\bar{q}\bmod(m)$ and $\eta(t)=1$. Define a character χ_2 of $Gal(L/K)$ by $\chi_2(s)=1$ and $\chi_2(t)=q^{1-d}\pmod m$. Then the fixed field of L by the kernel of χ_2 $(=\langle s\rangle)$ equals $K(\sqrt[d]{f})$. Furthermore, $\chi_2'(s)=\bar{q}\pmod m$ and $\chi_2'(t)=\overline{q^{d-1}}\pmod m$; $\chi_2'(st)=\overline{q^d}\equiv 1\pmod m$; thus the kernel of χ_2' is $\langle st\rangle$.

We claim that the fixed field of L by the kernel of χ_2' is $K(\sqrt[d]{nf})$; clearly, $s(\beta)=\zeta_d^{-1}\beta$, so $s(\sqrt[d]{n})=\zeta_d^{-1}\sqrt[d]{n}$; thus $st(\sqrt[d]{nf})=\sqrt[d]{nf}$; therefore, the fixed field of L by the kernel of χ_2' is $K(\sqrt[d]{nf})$. Set $\chi_2'=\chi_1$.

As before, A_i denotes the integral closure of A in L_i for $i=1,2$. Let $r_1=m$-rank of $(Cl_{L_1})_{\chi_1}$ and $r_2=m$-rank of $(Cl_{L_2})_{\chi_2}$. By investigating the local situation at infinity we can show that L_2/K is totally real and L_1/K is totally imaginary. From the Spiegelungssatz it follows that

$$-\delta_{\chi_2}\leqslant r_2-r_1\leqslant\delta_{\chi_1},$$

where $\delta_{\chi_2}=m$-rank of $(E_2^o)_{\chi_2}$, $\delta_{\chi_1}=m$-rank of $(E_1^o)_{\chi_1}$, and E_i^o is the group of primary units in E_{L_i} (i.e. the group of $u\in E_{L_i}$ such that $L_i(\sqrt[m]{u})/L_i$ is unramified for $i=1,2$).

For Theorem 2.3, we define some vector spaces as follows:

Definition 2.1. Let $\tilde{\Omega}$ be the subgroup (and sub G-module) of $L_2^\times/L_2^{\times m}$ consisting of the elements $\bar{\alpha}$ such that $\alpha^\delta\in\alpha^{\chi_2(\delta)}L_2^{\times m}$ for all $\delta\in Gal(L/K)$, i.e. $\tilde{\Omega}=\varepsilon_{\chi_2}(L_2^\times/L_2^{\times m})$, where ε_{χ_2} is the idempotent corresponding to the character χ_2, given by $\varepsilon_{\chi_2}=\frac{1}{|Gal(L/K)|}\sum_{\sigma\in G(L/K)}\chi_2(\sigma)\sigma^{-1}$.

Let $\tilde{C}'$ be the subgroup of $\tilde{\Omega}$ consisting of the elements $\bar{\alpha}$ such that the principal ideal generated by α in L_2 is the mth power of a fractional ideal $\mathscr{F}$ of L_2, i.e. $(\alpha) = \mathscr{F}^m$.

Let $\tilde{C}$ be the subgroup of $\tilde{C}'$ consisting of the elements $\bar{\alpha}$ such that $m | ord_{\wp_\infty}(\alpha)$ and

$$\alpha \cdot (\pi_{\wp_\infty})^{-\mathrm{ord}_{\wp_\infty}(\alpha)} \equiv X^m \pmod{\wp_\infty}$$

is solvable for every prime $\wp_\infty \in S_\infty(L_2)$.

Let $\tilde{\mathscr{E}}$ be the subgroup of $\tilde{C}'$ consisting of the elements which are representable by units of L_2, i.e. $\tilde{\mathscr{E}} = \tilde{C}' \cap (E_{L_2}/E_{L_2}^m)$.

The following Proposition 2.2 shows that Minkowski's Theorem on units holds for function fields as well, so we are able to determine the structure of the unit group of function fields modulo mth powers as a $\mathbb{Z}_m[G]$ module (G = Galois group).

Proposition 2.2. *Let* $G \stackrel{\mathrm{def}}{=} Gal(L_2/K) = \{\sigma_i | 1 \leqslant i \leqslant d\}$ *and* $\sigma_1 =$ *identity. Let* $S = S_\infty(L_2) = \{p_{\infty,1}, p_{\infty,2}, \ldots, p_{\infty,d}\}$ *and* $p_{\infty,i} = \sigma_i^{-1}(p_{\infty,1}) = p_{\infty,\sigma_i^{-1}}$ *for* $\sigma \in G, 1 \leqslant i \leqslant d$. $E(S)$ *is the S- unit group* $\{\alpha \in L_2^* | ord_p \alpha = 0, \forall p \notin S\}$.

Then there exists an S-unit $\varepsilon \in E(S)$ *such that the set of units* $\{\varepsilon^{\sigma_i} | 2 \leqslant i \leqslant d\}$ *is multiplicatively independent, hence generates a subgroup of finite index in the full group* $E(S)$. *In fact,* ε *is called a Minkowski unit.*

Proof. In fact, rank $E(S) = |S| - 1 = d - 1$ and $E_{L_2} = E(S)$. By the product formula we have

$$\prod_p |\varepsilon_s|_p = \prod_{i=1}^{d} |\varepsilon_s|_{p_{\infty,i}} = 1.$$

$|\varepsilon^{\sigma_i}|_{p_{\infty,1}} = |\varepsilon|_{p_{\infty,\sigma_i^{-1}}} = |\varepsilon|_{p_{\infty,i}}$ for $1 \leqslant i \leqslant d$.

Define a mapping

$$\phi : E(S) \to \mathbb{R}[G]$$

by $\phi(\varepsilon) = \sum_{i=2}^{d} \log |\varepsilon^{\sigma_i}|_{p_{\infty,1}} \sigma_i$. Then clearly, the kernel of ϕ is a finite group and the image of ϕ is in the augmentation ideal $I_{\mathbb{R}}$ of $\mathbb{R}[G]$ by the product formula. Thus, ϕ induces an isomorphism as $\mathbb{R}[G]$-modules

$$E(S) \otimes_{\mathbb{Z}} \mathbb{R} \simeq I_{\mathbb{R}}.$$

It follows that

$$E(S) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq I_{\mathbb{Q}}$$

as $\mathbb{Q}[G]$-modules, where $I_{\mathbb{Q}}$ is the augmentation ideal of $\mathbb{Q}[G]$. Hence, the proposition follows immediately. □

The result of the following Theorem 2.3 is a group-theoretical version of the Spiegelungssatz in cyclic function fields.

Theorem 2.3. *The $\mathbb{F}_m$-vector spaces $(Cl_{L_1}(m))_{\chi_1}, (Cl_{L_2}(m))_{\chi_2}, \tilde{\mathscr{E}}, \tilde{C}'$ and $\tilde{C}$ have the following properties*:

(i) *$\tilde{C}$ is isomorphic to $(Cl_{L_1}(m))_{\chi_1}$ as $\mathbb{F}_m$-vector spaces.*

(ii) *The sequence $1 \to \tilde{\mathscr{E}} \to \tilde{C}' \xrightarrow{\psi} (Cl_{L_2}(m))_{\chi_2} \to 1$ is exact,*

where ψ is a homomorphism $\psi : \tilde{C}' \to (Cl_{L_2}(m))_{\chi_2}$ defined by the following: If $\bar{\alpha} \in \tilde{C}'$ then $(\alpha) = \mathscr{F}^m$; then $\psi(\bar{\alpha})$ is the ideal class of $\mathscr{F}$.

(iii) *$\tilde{\mathscr{E}}$ is of dimension 1.*

(iv) *$\tilde{C}$ is a subspace of $\tilde{C}'$ of codimension less than or equal to 1.*

Proof. We show (i) $\tilde{C} \simeq (Cl_{L_1}(m))_{\chi_1}$ as $\mathbb{F}_m$-vector spaces.

Let $S_\infty(L_1)$ be a set of primes above ∞ which are in L_1 and $L_1^{A_1}$ be the maximal unramified elementary m-extension of L_1 in $L_{1_{\text{sep}}}$ where every $P_\infty \in S_\infty(L_1)$ splits completely. Let $\tilde{A}$ be the integral closure of A_1 in L and $L^{\tilde{A}}$ be the Hilbert class field of L with respect to $\tilde{A}$.

From the class field theory it follows that

$$Gal(L^{\tilde{A}}/L) \simeq Gal(L_1^{A_1}/L_1) \simeq Cl_{L_1}(m).$$

Let C be the subgroup of $L^\times/L^{\times m}$ consisting of the elements $\bar{\alpha}$ which satisfy the following conditions:

1. The principal ideal generated by α in L is the mth power of a fractional ideal $\mathscr{F}$ of L, i.e. $(\alpha) = \mathscr{F}^m$.
2. For every prime $\wp_\infty \in S_\infty(L)$,

$$m | ord_{\wp_\infty}(\alpha) \text{ and}$$

$$\alpha \cdot (\pi_{\wp_\infty})^{-\text{ord}_{\wp_\infty}(\alpha)} \equiv X^m \pmod{\wp_\infty} \quad \text{is solvable.}$$

Then $\varepsilon_{\chi_2} C = \tilde{C}$.

There is a non-degenerate bilinear pairing as follows:

$$Gal(L^{\tilde{A}}/L) \times C \to \mu_m,$$

$$< h, \bar{a} > = \frac{h(a^{1/m})}{a^{1/m}};$$

if $a \in C$, then $L(a^{1/m})/L$ is unramified everywhere and splits completely at every prime at infinity in $S_\infty(L)$; so $a^{1/m} \in L^{\tilde{A}}$; therefore the map is well-defined.

It is easy to verify that $L^{\tilde{A}}/L_1$ is Galois. In addition, $G(L^{\tilde{A}}/L)$ is normal in $G(L^{\tilde{A}}/L_1)$ since L/L_1 is normal; hence $G(L/L_1) = \langle s \rangle$ can act on $Gal(L^{\tilde{A}}/L_1)$ by conjugation: Taking $h \in G(L^{\tilde{A}}/L_1)$ and extending s to $\tilde{s} \in G(L^{\tilde{A}}/L), h^s = \tilde{s}h\tilde{s}^{-1}$, which is independent of the choice of $\tilde{s}$ since $G(L^{\tilde{A}}/L)$ is abelian. Then, applying Lemma 4.4 of [8], we have the following induced non-degenerate pairing:

$$\varepsilon_{\chi_1} Gal(L^{\tilde{A}}/L) \times \varepsilon_{\chi_2} C \to \mu_m. \tag{1}$$

From the class field theory it follows that

$$Gal(L^{\tilde{A}}/L) \simeq Cl_L(m).$$

Thus, we have the following isomorphisms as finite abelian groups:

$$(Cl_L(m))_{\chi_1} \simeq \varepsilon_{\chi_1} Gal(L^{\tilde{A}}/L) \simeq \varepsilon_{\chi_2} C = \tilde{C}. \tag{2}$$

In addition, applying Lemma 1.7 in [6], we obtain

$$(Cl_L(m))_{\chi_1} \simeq (Cl_{L_1}(m))_{\chi_1}. \tag{3}$$

Hence, it follows that $\tilde{C} \simeq (Cl_{L_1}(m))_{\chi_1}$ as $\mathbb{F}_m$- vector spaces.

Condition (ii) results essentially from the definitions. Now we show (iii). As shown in Proposition 2.2 Minkowski's Theorem holds for the case of function fields as well. We use the same notations as in Proposition 2.2. There is an exact sequence as follows:

$$1 \to E(S)^m \to E(S) \to L_2^\times / L_2^{\times m}.$$

Then $\mathscr{E} \stackrel{\text{def}}{=} E(S)/E(S)^m \hookrightarrow L_2^\times / L_2^{\times m}$; hence, $\mathscr{E}(\chi_2) \hookrightarrow \tilde{\Omega} = (L_2^\times / L_2^{\times m})(\chi_2)$ and in fact, $\mathscr{E}(\chi_2) \hookrightarrow \tilde{C}' \subset \tilde{\Omega}$. Therefore, $\tilde{\mathscr{E}} = \mathscr{E}(\chi_2)$. By applying Proposition 2.2 we have

$$E(S) \otimes \mathbb{Z}_m \simeq (\mathbb{Z}[G]/(N)) \otimes \mathbb{Z}_m \simeq \mathbb{Z}_m[G]/(N) \simeq \oplus_\psi (\mathbb{Z}_m[G])\varepsilon_\psi,$$

where ψ is a non-trivial character of G, ε_ψ is an idempotent corresponding to ψ, and (N) is an ideal generated by the norm of G.

Hence, $(E(S)/E(S)^m) \otimes \mathbb{Z}/m\mathbb{Z} \simeq \oplus_\psi (\mathbb{Z}/m\mathbb{Z}[G])\varepsilon_\psi$ Consequently, $\tilde{\mathscr{E}} = \mathscr{E}(\chi_2) = (E(S)/E(S)^m \otimes \mathbb{Z}/m\mathbb{Z})(\chi_2) = (\mathbb{Z}/m\mathbb{Z}[G])\varepsilon_{\chi_2}$, which is 1-dimensional as $\mathbb{Z}/m\mathbb{Z}$-vector space.

Now it remains to prove (iv). Since every prime in S_∞ splits completely in L_2, the completion of L_2 at $\wp_\infty \in S_\infty(L_2)$, denoted by $(L_2)_{\wp_\infty}$, is equal to K_∞. In addition,

we know the structure of $K_\infty^\times$:

$$K_\infty^\times = \langle \pi_\infty \rangle \times \mu_{q-1} \times U_\infty^{(1)},$$

where μ_{q-1} is a set of $(q-1)$th roots of unity and $U_\infty^{(1)} = 1 + \langle \pi_\infty \rangle$ is a set of principal local units. In fact, $\langle \pi_\infty \rangle = \langle T^{-1} \rangle$.

We define a natural map

$$\psi : \tilde{C}' \to (L_2)_{\wp_\infty}^\times / (L_2)_{\wp_\infty}^{\times m}$$

by $\psi(\alpha) = \bar{\alpha}$ (mod mth powers). Then from the definition of $\tilde{C}$ it follows that the kernel of ψ is equal to $\tilde{C}$. Since $(L_2)_{\wp_\infty} = K_\infty, m$ is prime to p and $U_\infty^{(1)}$ is a p-group, we have the following isomorphisms:

$$(L_2)_{\wp_\infty}^\times / (L_2)_{\wp_\infty}^{\times m} \simeq \langle \pi_\infty \rangle / \langle \pi_\infty \rangle^m \simeq \mathbb{Z}/m\mathbb{Z}.$$

Therefore,

$$\tilde{C}'/\tilde{C} \simeq \textit{Image of } \psi \subseteq \mathbb{Z}/m\mathbb{Z},$$

which shows that $\tilde{C}$ is a subspace of $\tilde{C}'$ of codimension $\leqslant 1$. □

Corollary 2.4. $r_2 = r_1 - 1 + \textit{codim}\ \tilde{C}$.

3. Compatibility in the case of cyclic function fields

Friedman and Washington [3] proposed the conjecture which is analogous to Cohen–Lenstra heuristics for hyperelliptic curves over finite fields. Cohen–Lenstra conjectures concern Galois extensions of the rational field $\mathbb{Q}$. Cohen and Martinet [1] generalized in 1990 Cohen–Lenstra conjectures to arbitrary extensions of number fields, even to the non-Galois case. We obtain the function field analogue of Cohen–Martinet heuristics by generalizing Friedman–Washington's conjectures for the function field analogue of the Cohen–Lenstra heuristics (for more details, we can refer to [5]). We will use the generalized Friedman and Washington's conjectures in this section.

We have $\Gamma \stackrel{\text{def}}{=} Gal(L_2/K) \simeq \mathbb{Z}/d\mathbb{Z}$; hence, $\mathcal{O}_\Gamma$, the maximal order in the ring $\mathbb{Q}[\Gamma]/(\sum_{\sigma\in\Gamma}\sigma)$ is equal to $\mathbb{Z}[\zeta_d]$. $Cl_{L_2}(m)$ is a semisimple algebra over $\mathbb{F}_m$ and the exponent d of $G(L_2/K)$ divides $m-1$; hence, every irreducible m-adic character is 1-dimensional; we have the following decomposition:

$$Cl_{L_2}(m) \simeq (Cl_{L_2}(m))_\chi \oplus (Cl_{L_2}(m))_{\chi^2} \oplus \cdots \oplus (Cl_{L_2}(m))_{\chi^{d-1}},$$

where χ is a generator of a character group of Γ (and χ is a m-adic character of Γ).

As $m \equiv 1 \pmod{d}$, (m) splits completely in $\mathcal{O}_\Gamma$. Let $\wp_1, \wp_2, \ldots, \wp_{d-1}$ be prime ideals in $\mathcal{O}_\Gamma$ above (m). Then

$$Cl_{L_2}(m) \simeq Cl_{L_2}(\wp_1) \oplus Cl_{L_2}(\wp_2) \oplus \cdots \oplus Cl_{L_2}(\wp_{d-1}).$$

Comparing both decompositions above, we have

$$(Cl_{L_2}(m))_\chi \simeq Cl_{L_2}(\wp_i)$$

for some $i, 1 \leqslant i \leqslant d-1$.

From the function field of Cohen–Lenstra heuristics, we have the following result:

$$\begin{aligned} &P(m - \text{rank of } (Cl_{L_1}(m))_{\chi_1} = a) \\ &= P(\wp_i - \text{rank of } Cl_{L_1}(\wp_i) = a) \\ &= (N\wp_i)^{-a^2} \eta_\infty(\wp_i)/(\eta_a(\wp_i)\eta_a(\wp_i)), \text{ where } \eta_a(\wp_i) = \prod_{1 \leqslant i \leqslant a} (1 - N(\wp_i)^{-i}). \\ &= m^{-a^2} \prod_{i \geqslant 1} (1 - m^{-i}) \prod_{1 \leqslant i \leqslant a} (1 - m^{-i})^{-2}, \text{ since } N\wp_i = m. \end{aligned}$$

Therefore, we have

$$P(r_1 = a) = m^{-a^2} \prod_{i \geqslant 1} (1 - m^{-i}) \prod_{1 \leqslant i \leqslant a} (1 - m^{-i})^{-2}. \tag{4}$$

In a similar way, we obtain the probability concerning L_2 as follows:

$$P(r_2 = a) = m^{-a(a+1)} \prod_{i \geqslant 1} (1 - m^{-i}) \prod_{1 \leqslant i \leqslant a} (1 - m^{-i})^{-2} (1 - m^{-(a+1)})^{-1}. \tag{5}$$

We note that the probabilities in (4) and (5) are conjectural. Now, by using the Spiegelungssatz, we show the coherence of these conjectures concerning m-ranks of class groups of cyclic function fields. We begin with assuming that the conjectured probability about the m-rank of the class group of real cyclic function field L_2 is true. Then by using the Spiegelungssatz, we deduce the probability about the m-rank of the class group of imaginary cyclic function field L_1. Under one plausible extra assumption below in (6) we will show that the result of the probability about the m-rank of the class group of imaginary cyclic function field L_1 (which is independent of Cohen–Lenstra conjectures) is exactly equal to the conjectural statement about the m-rank of the class group of imaginary cyclic function field L_1 given by Cohen–Lenstra heuristics.

From Corollary 2.4 we have

$$r_2 = r_1 - 1 + d,$$

where d is the codimension of $\tilde{C}$ in $\tilde{C}'$. Since codim $\tilde{C} \leqslant 1$, d is either 0 or 1. Hence, we have only two cases, either $d = 0, r_2 = r_1 - 1$ or $d = 1, r_2 = r_1$.

In order to show the compatibility, we need the conditional probability that d equals 0 knowing that r_2 equals β. We thus make the following:

Assumption.

$$P(d = 0 | r_2 = \beta) = 1/m^{\beta+1}. \tag{6}$$

By using the map ψ used for the proof of (iv) of Theorem 2.3, we can make this assumption plausible as follows:

$$\psi : \tilde{C}' \to (L_2)^{\times}_{\wp_\infty} / (L_2)^{\times m}_{\wp_\infty}$$

is defined by $\psi(\alpha) = \bar{\alpha}$ (mod mth powers). We know that the kernel of ψ equals $\tilde{C}$ and

$$(L_2)^{\times}_{\wp_\infty} / (L_2)^{\times m}_{\wp_\infty} \simeq \langle \pi_\infty \rangle / \langle \pi_\infty \rangle^m \simeq \mathbb{Z}/m\mathbb{Z}.$$

Hence, d (= the codimension of $\tilde{C}$ in $\tilde{C}'$) equals zero if and only if ψ is the zero map. If we assume that $r_2 = \beta$, then $\tilde{C}'$ has m-rank equal to $\beta + 1$, so there are possible $m^{\beta+1}$ maps from $\tilde{C}'$ to $(L_2)^{\times}_{\wp_\infty} / (L_2)^{\times m}_{\wp_\infty}$; if we assume that ψ has an equal chance of being any of these maps, then the probability that ψ is the zero map, given that $\tilde{C}'$ has m-rank equal to $\beta + 1$, is $1/m^{\beta+1}$.

From assumption (6), it therefore follows that

$$P(d = 1 \,|\, r_2 = \beta) = 1 - 1/m^{\beta+1}. \tag{7}$$

Now we want to deduce the probability about the m-rank of the class group of imaginary cyclic function field L_1, by applying the Spiegelungssatz (Corollary 2.4) and using the conjectured probability about the m-rank of the class group of real cyclic function field L_2, i.e. (5).

$$\begin{aligned}
&P(r_1 = a) \\
&\quad = P(d = 0, r_2 = a - 1) + P(d = 1, r_2 = a) \\
&\quad = P(r_2 = a - 1)P(d = 0 \,|\, r_2 = a - 1) + P(r_2 = a)P(d = 1 \,|\, r_2 = a) \\
&\quad = m^{-a(a-1)}\eta_\infty(m) \prod_{i=1}^{i=a-1} (1 - m^{-i})^{-2}(1 - m^{-a})^{-1}m^{-a} \\
&\qquad + m^{-(a+1)a}\eta_\infty(m) \prod_{i=1}^{i=a} (1 - m^{-i})^{-2}(1 - m^{-(a+1)})^{-1}(1 - m^{-(a+1)})
\end{aligned}$$

by applying (5), (6) and (7).

$$\begin{aligned}
&= \eta_\infty(m) \prod_{i=1}^{i=a} (1-m^{-i})^{-2} [m^{-a(a-1)}(1-m^{-a}) l^{-a} \\
&\quad + m^{-a(a+1)}(1-m^{-(a+1)})(1-m^{-(a+1)})^{-1}] \\
&= \eta_\infty(m) \prod_{i=1}^{i=a} (1-m^{-i})^{-2} [m^{-a^2} - m^{-a^2-a} + m^{-a^2-a}] \\
&= m^{-a^2} \eta_\infty(m) \prod_{i=1}^{i=a} (1-m^{-i})^{-2}
\end{aligned}$$

We thus find the probability that m-rank of $(Cl_{L_1}(m))_{\chi_1}$ equals a as follows:

$$P(r_1 = a) = m^{-a^2} \eta_\infty(m) \prod_{i=1}^{i=a} (1-m^{-i})^{-2}$$

which is exactly the same value that we obtained in (4) for the function field analogue of Cohen–Lenstra heuristics. Moreover, in a similar way as above we can deduce the probability about L_2, i.e. $P(r_2 = a)$ by assuming that the conjectured probability about L_1, i.e. $P(r_1 = a)$ is true and using the Spiegelungssatz for cyclic function fields. Then the deduced probability about L_2, i.e. $P(r_2 = a)$ can be shown to be precisely the same as the conjectured probability about L_2, i.e. (5). We have shown that the conjectural probabilities about m-ranks of Cl_{L_1} and Cl_{L_2} are compatible with the Spiegelungssatz.

Acknowledgments

I express my gratitude to Dr. Michael Rosen for his invaluable comments, and especially to a referee for very helpful suggestions for the clarity of the paper.

References

[1] H. Cohen, J. Martinet, Étude heuristique des groupes de classes des corps de nombres, J. Reine Angew. Math. 404 (1990) 39–76.
[2] P. Dutarte, Compatibilité avec le Spiegelungssatz de probabilités conjecturales sur le p-rang du group des classes, Théorie des nombres (Besançon 1983-1984), Exp. No. 4, 11pp.
[3] E. Friedman, L.C. Washington, On the distribution of divisor class groups of curves over a finite field, Théorie des nombres (Quebec 1987), pp. 227–239.
[4] C. Friesen, A special case of Cohen–Lenstra heuristics and in function fields, CRM Proceedings Lecture Notes, American Mathematical Society, Providence, RI, Vol. 19, 1999, pp. 99–105.
[5] Y. Lee, Cohen–Lenstra heuristics and the Spiegelungssatz, Dissertation, Brown University, 1999.
[6] Y. Lee, Cohen–Lenstra heuristics and the Spiegelungssatz; number fields, J. Number Theory 92 (2002) 37–66.

[7] H.W. Leopoldt, Zur Struktur der l-Klassengruppe galoisscher Zahlkörper, J. Reine Angew. Math. 199 (1958) 165–174.
[8] R. L. Long, Algebraic Number Theory, Marcel Dekker, New York and Basel, 1977.
[9] M.I. Rosen, *S*-units and *S*-class group in algebraic function fields, J. Algebra 26 (1973) 98–108.
[10] M.I. Rosen, The Hilbert class field in function fields, Expo. Math. 5 (1987) 365–378.
[11] J.K. Yu, Toward a proof of the Cohen–Lenstra conjecture in the function field case, preprint.

Further reading

C. Chevalley, Introduction to the theory of algebraic functions of one variable, Mathematical Surveys and Monographs, Vol. VI, American Mathematical Society, 1951.
H. Cohen, H.W. Lenstra, Heuristics on Class Groups of Number Fields, Lecture Notes in Mathematics, Vol. 1068, Springer, Berlin, 1984, pp. 33–62.
H. Cohen, J. Martinet, Class groups of number fields: numerical heuristics, Math. Comput. 48 (1987) 123–137.
M. Deuring, Lectures on the Theory of Algebraic Functions of One Variable, Springer, Berlin, 1973.
G. Gras, Extensions abéliennes non ramifiées de degré premier d'un corps quadratique, Bull. Soc. Math. France 100 (1972) 177–193.
M. Krasner, Sur la representation exponentielle dans les corp relativement galoisien de nombres *p*-adique, Acta Arith. 3 (1939) 133–173.
J. Neukirch, Class Field Theory, Springer, Berlin, 1986.
R.S. Pierce, Associative Algebras, Springer, New York, 1982.
M.I. Rosen, An elementary proof of the local Kronecker–Weber theorem, Trans. Amer. Math. Soc. 265 (2) (1981) 599–605.
J.P. Serre, Local Fields, Springer, New York, 1980.
L.C. Washington, Introduction to Cyclotomic Fields, Springer, New York, 1997.